ABSTRACT

To prevent piracy, audiovisual content is encrypted prior to transmission to consumers. A low-cost, high-security cryptographic rights module (such as a smartcard) enables devices such as players/displays to decode such content. Security-critical functions may be performed by the cryptographic module in a manner that allows security compromises to be addressed by upgrading or replacing cryptographic modules, thereby avoiding the need to replace or modify other (typically much higher-cost) components. The security module contains cryptographic keys, which it uses to process rights enablement messages (REMs) and key derivation messages (KDMs). From a REM and KDM, the security module derives key data corresponding to content, uses public key and/or symmetric cryptography to re-encrypt the derived key data for another device, and provides the re-encrypted key data to the decoding device. The decoding device then uses cryptographic values derived from the re-encrypted key data to decrypt the content.